

25th Anniversary

**NYS CYBERSECURITY
CONFERENCE**



June 6-7, 2023

Presented By



**Office of Information
Technology Services**



SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY
State University of New York



TABLE OF CONTENTS

| | |
|-------------------------------------|-----|
| Conference Co-Hosts..... | 4-5 |
| Keynotes | 6-7 |
| Agenda At-A-Glance | 8-9 |
| Session Descriptions..... | 11 |
| Sponsors | 25 |
| Exhibitors..... | 33 |
| Booth Assignments & Floor Plan..... | 43 |



Empire State Plaza Public Space WIFI:
ESP-Public Wifi

WELCOME LETTER

June 6, 2023

Dear Attendee:

Welcome to the Silver Anniversary of the New York State Cybersecurity Conference!

The 25th New York State Cybersecurity Conference (NYSCSC) and the 17th Annual Symposium on Information Assurance (ASIA) is hosted by the New York State Office of Information Technology Services (ITS), the School of Business at the University at Albany, State University of New York, and The NYS Forum, Inc. We are pleased to offer you an agenda filled with innovative and information-packed sessions and the opportunity to learn alongside a nationwide cohort of peers who share your passion for cybersecurity.

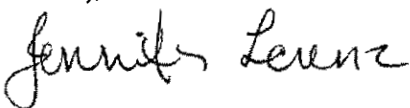
Since our inaugural conference, held in 1998, information technology and cybersecurity have grown to become an extensive area of operational expertise required for every governmental and business entity. Today, the need exists for the latest reports and the most innovative technologies, as well as experts trained to apply these resources to best protect their organizations from an ever-growing list of cyber threats.

New York State, under Governor Kathy Hochul, has fostered some of the most robust cybersecurity operations in the nation. Every day New York is focused on the challenges that pose serious risks to our information, systems, networks, and personal data.

Cybersecurity is everyone's responsibility and together we can make our environment safer. Whether you are new to the field, or have years of experience, this conference offers relevant lessons for all attendees. With more than 50 sessions, the conference provides the latest on security evolution, current threat landscape, and cybersecurity strategy. Take full advantage of your time at this conference. Network with your peers, learn from the presenters and exhibitors, be motivated by the keynotes, fully immerse yourself in the interactive training, and be inspired by what we can learn when we work collaboratively.

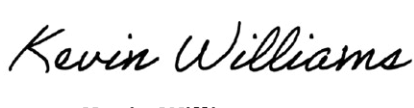
Thank you for attending the conference and understanding the importance of cybersecurity today. We hope you leave with the knowledge and inspiration to continue to help strengthen our collective future. Your commitment to a more secure tomorrow is an inspiration for us all. Enjoy the conference!

Sincerely,



Jennifer Lorenz

Acting Chief Information Officer
NYS Office of Information Technology Services.



Kevin Williams

Interim Dean, School of Business
University at Albany



Fran Reiter

Executive Director
NYS Forum



**Office of Information
Technology Services**



SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY
State University of New York



CONFERENCE CO-HOSTS



Jennifer Lorenz

Acting Chief Information Officer
New York State Office of Information Technology Services

Jennifer Lorenz has more than 20 years of experience as a leader and operational manager of information technology systems. Previously the ITS Deputy Chief Information Officer for Operations, Jenn has taken on the role of Acting Chief Information Officer. In this role, Jenn oversees the operations of the entire agency, including governing the framework for introducing new systems, programs and technologies to New York State agencies, as well as ensuring alignment between IT, client business strategies and financial objectives.

Prior to her role as Deputy CIO for Operations, Jenn led the NYS ITS Chief Portfolio Office. Her technical expertise has led to numerous service improvements and statewide technology transformation efforts. She is a results-oriented leader who advocates for leveraging technology to solve business problems and create process efficiencies.

Jenn has been with ITS since the agency's inception in 2012. She previously served in the United States Air Force. Jenn holds a bachelor's degree in business management from Empire State College and an ITIL Foundations certification.



Kevin Williams

Interim Dean, School of Business
University at Albany

Kevin Williams is Interim Dean of the School of Business at the University at Albany. Previously, he served for 13 years as Vice Provost and Dean of Graduate Education at Albany. Dr. Williams is a Collins Fellow and Professor of Industrial-Organizational Psychology at the University, and was the recipient of the President's and Chancellor's Excellence Awards in Teaching in 2007. He received his master's and Ph.D. degrees from the University of South Carolina, and his bachelor's from SUNY Plattsburgh. Williams' research and teaching interests focus on the application of psychology to organizational settings. He has over 60 publications mainly in the areas of organizational behavior, human resource management, and psychological aspects of cybersecurity.

CONFERENCE CO-HOSTS



Fran Reiter

Executive Director
NYS Forum

Following an early career in theater and film production and a 15-year career as a marketing executive in the television industry, Fran Reiter served as NYC Deputy Mayor for Planning and Community Relations and, subsequently, for Economic Development and Planning during Mayor Rudolph Giuliani's first term. Her many accomplishments include authoring and overseeing the implementation of the Lower Manhattan Revitalization Plan, negotiating the citywide Adult Use Rezoning and the community agreement that led to the first Williamsburg rezoning, and leading the restructuring of the NYC Division of AIDS Services.

Fran left government service to run Mayor Giuliani's successful 1997 re-election campaign then returned to the private sector, serving as President and CEO of the NYC Convention and Visitors Bureau (now NYC & Company) and Executive Director of the Joseph Papp Public Theater/NY Shakespeare Festival. In 2003, she was a founding partner of lobbying firm Reiter/Begun Associates which merged with J. Adams Consulting in 2011, creating the Reiter Giuliani Group, LLC, now RG Group. With 40 years of private and public sector expertise, Fran provides government relations, strategic advisement, and lobbying services to a diverse array of businesses and non-profit organizations.

At the request of Governor Andrew Cuomo, Fran returned to public service in November 2012 to serve as Executive Deputy Director of State Operations, overseeing all state agency operations and the realization of the Governor's major enterprise-wide initiatives, including the implementation of the Office of Information Technology Services, the Business Service Center, and the eLicensing program.

Fran returned to RG Group in September 2014 to head the firm's Albany office. In early 2021, she retired from RG Group and established Reiter Consulting, LLC, providing strategic advisement to businesses and organizations doing or seeking to do business with New York City and State government.

Fran has been an adjunct professor at New York University and the Baruch College School of Public Affairs. Additionally, she has been a guest lecturer at NYU, the New School for Social Research, and Columbia University.

Fran is a native New Yorker and holds a B.S. in Public Affairs from the City University of New York.

DAY 1 KEYNOTE – JUNE 6

Cyber Resilience for the Public

Government entities provide an array of services for the public – from business to social, and everything in between. Many of these services are the backbone of a functioning society. New Yorkers have become accustomed to the benefits offered by these services and may not realize the sheer impact they have on our livelihood. It is our duty to work backwards from New York residents to architect cyber resilience and protect the services they require.



Quiescence Phillips

Amazon Web Services

Security Technical Program Manager

Former Deputy CISO, City of New York and Head of Threat Management,
NYC Cyber Command

Quiescence is a transformational leader, whose creative strategies and execution has helped build impactful and innovative teams in the Cybersecurity industry. With 15 years of experience spanning private and public sector, she brings a wealth of knowledge and experience to her work. She also brings her inspirational and unique teaching style to a large body of students through her role as an adjunct professor at NYU Tandon School of Engineering and co-founder of non-profit EdTech, JOURNi.

Quiescence's leadership, in her role as Deputy CISO for the City of New York, yielded the first of its kind centralized Threat Management program for a municipality. She is now making Security AWSome at the largest cloud provider, Amazon Web Services (AWS).

Quiescence has been recognized as "Best of New York" by City Tech Foundation, published in *Women Know Cyber: 100 Fascinating Females Fighting Cybercrime*, *Tribe of Hackers: Blue Team Edition*, *97 Things Every Information Security Professional Should Know*, and awarded Security Team of the Year for public sector by FireEye.

DAY 2 KEYNOTE – JUNE 7

Breaking Hearts and Taking Tether



“HODL” with FBI Albany on a cautionary tale of online romance and revenge. Bring your AI Buzzword Bingo card for our look at a future with generative AI as an attacker resource.

Janeen DiGuseppi

Director Christopher Wray has named Janeen DiGuseppi as the Special Agent in Charge of the Albany Field Office in Albany, New York. Most recently, DiGuseppi was the Deputy Assistant Director of the FBI’s Training Division.

DiGuseppi joined the FBI as a Special Agent in 1999 and was first assigned to the Salt Lake City Field Office, where she worked violent crime, drug, and public corruption violations.

In 2008, DiGuseppi was promoted to Assistant Legal Attaché in Baghdad and supervised the FBI’s Major Crimes Task Force. She returned to Salt Lake City in 2009 and was assigned to the DEA’s Drug Diversion Task Force until she was promoted to Supervisory Special Agent in 2010 as the FBI’s biometric lead in Kabul, Afghanistan.

DiGuseppi was assigned to the Memphis Field Office in Tennessee in 2012, where she supervised the civil rights and public corruption programs and the Violent Crimes Against Children/Child Exploitation Task Force.

In 2014, she was promoted to Assistant Section Chief of the Public Corruption and Civil Rights Section in the Criminal Investigative Division at FBI Headquarters in Washington, D.C. She later served as the Chief of Staff to the division’s Assistant Director. In 2016, she was named Assistant Section Chief of the Transnational Organized Crime - Eastern Hemisphere Section, where she managed domestic and international programs focused on organized crime and major theft.

DiGuseppi was named Assistant Special Agent in Charge in the Denver Field Office in 2017, with oversight of the intelligence and surveillance programs, the Rocky Mountain Regional Computer Forensic Laboratory, and the Wyoming resident agencies.

In 2019, DiGuseppi was selected as Section Chief of the FBI Training Division’s Curriculum Management Section, and promoted to Deputy Assistant Director in 2020.

DiGuseppi earned a bachelor’s degree from the University of Central Florida, a master’s degree from Western New England College, and a master’s degree from Florida International University. Prior to joining the Bureau, DiGuseppi served as an officer in the United States Air Force.

David Hinsdale

David currently serves as a Special Agent assigned to the cyber squad in the FBI Albany Field Office. He investigates computer intrusions from both the criminal and national security perspective. His work covers a diverse range of cyber-criminal activities to include Initial Access Vendors, Ransomware, BECs, Cyberstalking/Harassment, Credit Card Skimming, Identity Theft, and Cryptocurrency Fraud. David is also an FBI Digital Evidence Technician with multiple GIAC certifications and has been a Certified Public Accountant for ten years.

Roderick Link

Roderick has served as one of FBI Albany Division’s subject matter experts on digital forensics, cryptanalysis, network, memory and malware analysis in support of FBI operations and computer intrusion investigations. His recent major deployments include containing attackers accessing Super Bowl 2020 infrastructure, combating the SunBurst backdoor at U.S. federal agencies, and assisting with the international arrest of a subject in the US Navy’s largest ever public corruption investigation.

AT-A-GLANCE SCHEDULE, DAY 1: JUNE 6, 2023

| | | | | | | | | | | |
|-------------------|--|--|---|---|--|---|------------------|----------------------|----------------|----------------|
| 8:00am – 4:15pm | New York State Cybersecurity Conference Convention Hall | | | | | | | Tuesday June 6, 2023 | | |
| 9:00am – 10:30am | Welcome Address Keynote: "Cyber Resilience for the Public" Quiescence Phillips, Amazon Web Services, Security Technical Program Manager Former Deputy CISO, City of New York and Head of Threat Management, NYC Cyber Command | | | | | | | | | |
| 10:30am – 11:00am | Visit the Exhibitors (Terabyte Sponsor Demo: Fortinet 10:35am-10:55am) | | | | | | | | | |
| 11:00am – 11:50am | Zero Trust | | Managing AI | | Security Evolution | | Data Protection | Threat Landscape | ASIA | |
| | What is Zero Trust? | Case studies applying Machine-Learning in Cybersecurity | Building Cyber Resilience: Why Does it Matter and How Can You Get Started? | Why a Whole of Government Security Strategy protects all New Yorkers | 2023 Verizon Data Breach Investigations Report | Understanding Security Behavior | | | | |
| | Jeffrey Baez Splunk | Eric Dull Jeffery Janies Deloitte | Jim Richberg Fortinet | NYS Forum Information Security Workgroup | Neal Maguire Verizon Cyber Security Consulting | Development of Gig-Work Deviance Scale Creating a Balance between Monitoring Practices and Flexible Work Arrangements | | | | |
| 11:50am – 1:00pm | Meeting Room 4 | | Meeting Room 2-3 | | Meeting Room 1 | | Meeting Room 5 | | Meeting Room 6 | Meeting Room 7 |
| 1:00pm – 1:50pm | Lunch on your own and Visit the Exhibitors | | | | | | | | | |
| | Zero Trust Cybersecurity Strategy for Government IT Leaders - How to Stay Ahead of the New Cyber Battleground | How AI Embeds Human Bias and Distorts Our Decision Making | Beyond Layers: Achieving Holistic Cybersecurity through Tool Integration | How I Learned to Stop Worrying and Love My AI Overlords: Ethics and AI in Data Protection | Threat Landscape and Resources | Privacy Breaches | | | | |
| | Tommy John VMWare | Antony Haynes Albany Law | Ryan Young Vandis | F. Paul Greene Harter Secrest & Emery, LLP | Elijah Cedeno MSCAC | Investigating HIPAA Cybersecurity & Privacy Breach Compliance Reporting during COVID-19 Privacy Paradox: Is it really a paradox? | | | | |
| 1:50pm – 2:10pm | Meeting Room 4 | | Meeting Room 5 | | Meeting Room 1 | | Meeting Room 2-3 | | Meeting Room 6 | Meeting Room 7 |
| 2:10pm – 3:00pm | Visit the Exhibitors (Megabyte Sponsor Demo: Cisco 1:55pm-2:05pm) | | | | | | | | | |
| | How Breaches Should Shape Your Zero Trust Strategy | AI in Cybersecurity: Navigating the Hype and Making Informed Decisions | A Brave New World: An Exploratory Look into the Next Century of Hacking and Cybercrime Tactics | Data Security: Common Misconceptions with Immutability & Recovery Managing Endpoint Risk at Scale | Business Email Compromises: An Evolving Attack | Active Defense | | | | |
| | Jeremiah Salzberg CDWG | Dean Maloney GreyCastle Security | Tyler Wrightson Leet Cyber Security | Liam Kerns Tanium Shawn McElhinney Rubrik, Inc. | Courtney Dayter Jamie Vendel Kroll Cyber Risk | Honey pots and Honeypotokens in Active Defense Exploiting hacker biases to Thwart Hackers | | | | |
| 3:00pm – 3:20pm | Meeting Room 4 | | Meeting Room 2-3 | | Meeting Room 6 | | Meeting Room 5 | | Meeting Room 1 | Meeting Room 7 |
| 3:20pm – 4:15pm | Visit the Exhibitors (Megabyte Sponsor Demo: Deloitte 3:05pm-3:15pm) | | | | | | | | | |
| | An Introduction to Zero Trust Architecture | AI-Machine Learning-Data Management Governance & Controls Cloud Computing Best Practices: CNY Quantum Valley | ChatGPT – Yes, It Generates Code...but Is It Secure? Leveraging Machine Learning and Artificial Intelligence tools with Application Security Scanning | The Five Essentials of Ransomware Prevention | Uncover the Online Identity Threat Landscape and Path to Outsmart Risk | Cybercrime and Hacking | | | | |
| | Richard Conklin Accenture | Pentagon-USAF--USSF Ventures Spanning Air-Space- Cyberspace-Outer Space | Christopher Wysopal Veracode | Chris Jensen Tenable | George Freeman LexisNexis Risk Solutions | Improving Ethics Surrounding Collegiate-Level Hacking Education Investigating Cybercrime Using Code Authorship Analysis & 4P Forensic Conceptual Model | | | | |

AT-A-GLANCE SCHEDULE, DAY 2: JUNE 7, 2023

| New York State Cybersecurity Conference | | | | | | Wednesday June 7, 2023 |
|--|---|--|--|--|--|---|
| Convention Hall Keynote: "Breaking Hearts and Taking Tether" SAC Janeen DiGuseppi, SA David Hinsdale and CS Roderick Link, Albany FBI | | | | | | |
| 9:00am – 10:30am | | | | | | |
| 10:30am – 11:00am | Visit the Exhibitors (Terabyte Sponsor Demo: Fortinet 10:35am-10:55am) | | | | | |
| 11:00am – 11:50am | Defend & Protect The Importance of Incident Response Testing: This is NOT a Drill Daniel J. Altieri Laura K Schwalbe Harter Secrest & Emery, LLP | Compliance How Organizational Culture Impacts Compliance! Robert Adams iSecure LLC | Cyber Industry We Need a Compliance Control for Retaining Cybersecurity Professionals Diedre Diamond CyberSn | Cyber Strategy Resilience in a Cyber World—Three Critical Steps Towards a Mature Cyber Security Program Ryan Ettl Infoblox | Cloud Security Cloud Security...On the Cheap Randy Wheeler Christie Hall NYSTEC | ASIA Vulnerability Assessments Reliability of CVSS Scores in influencing security decisions |
| | Meeting Room 6 | Meeting Room 1 | Meeting Room 4 | Meeting Room 5 | Meeting Room 2-3 | Meeting Room 7 |
| 11:50am – 1:00pm | Lunch on your own and Visit the Exhibitors | | | | | |
| 1:00pm – 1:50pm | DevSecOps Explained Neil Pathare Synopsis | Number One Risk: Not Knowing your Asset Inventory Aaron Sanderson JANUS Associates | Methods and Tools to Help Grow and Keep Current Cyber Employees Susie Kendis Mara Patashnik Deloitte | Building Stronger Cybersecurity Communities: Driving Awareness and Training for a More Secure Digital World Kiran Bhujle Shahryar Shaghaghi SVAM International | Trends in Cloud Security Sailesh Gadia KPMG LLP | Phishing and Deception Too Much of a Good Thing: Examining Politeness Cues on Phishing Email Detection Beyond the Human Eye: Comprehensive Approaches to AI Text Detection |
| | Meeting Room 1 | Meeting Room 6 | Meeting Room 4 | Meeting Room 5 | Meeting Room 2-3 | Meeting Room 7 |
| 1:50pm – 2:10pm | Visit the Exhibitors (Megabyte Sponsor Demo: Deloitte 1:55pm-2:05pm) | | | | | |
| 2:10pm – 3:00pm | Cyber Defense Lessons from Ukraine Anita Biernat Utica University | Privacy Primer: Tips for Building, or Updating, Your Privacy Program Michelle Warner Jeffrey Wilson NYSTEC | Cyber Crime — Challenges and Solutions Carl Mazzanti eMazzanti Technologies | How Organizations "Stay Ready So You Don't Have to Get Ready" Erik Gaston Tanium | Digital Identity Making Sense of The Wild West of Digital Identity Ames Fowler Marcin Zimny ForgeRock | Covert Channels Introducing a Novel Covert Channel Into Backgammon COVERT CHANNELS IN CRYPTIC CROSSWORDS |
| | Meeting Room 6 | Meeting Room 1 | Meeting Room 4 | Meeting Room 5 | Meeting Room 2-3 | Meeting Room 7 |
| 3:00pm – 3:20pm | Visit the Exhibitors (Megabyte Sponsor Demo: Cisco 3:05pm-3:15pm) | | | | | |
| 3:20pm – 4:15pm | The Three Pillars of Email Authentication Joseph Martino Nicolas Villacis Vukadinovic Spruce Technology | What Do the New FTC Safeguard Rules Require You to Do in 2023? John Bruggeman CBTS | Anatomy of a Cyber Attack Dennis O'Connell Custom Computer Specialists | Creating a Cybersecurity Roadmap for Schools to Protect K-12 Students, Teachers and Parents Richard Cocchiara Cxo Expertise | How to Secure Active Directory: Best Practices for Detection, Remediation, and Recovery Steve Walker Semperis | Covert Channels Pragmatic Study of MQTT 5.0 Network Covert Channels |
| | Meeting Room 4 | Meeting Room 1 | Meeting Room 6 | Meeting Room 5 | Meeting Room 2-3 | Meeting Room 7 |

Sponsor Demonstration Schedule

June 6:

10:35am-10:55am

Terabyte Sponsor Fortinet

Booth #15-16, 56

1:55pm-2:05pm

Megabyte Sponsor Cisco

Booth #6-7

3:05pm-3:15pm

Megabyte Sponsor Deloitte

Booth #54-55

June 7:

10:35am-10:55am

Terabyte Sponsor Fortinet

Booth #15-16, 56

1:55pm-2:05pm

Megabyte Sponsor Deloitte

Booth #54-55

3:05pm-3:15pm

Megabyte Sponsor Cisco

Booth #6-7



ALBANY LAW SCHOOL
ONLINE GRADUATE PROGRAMS

Be the bridge.

**EXPAND YOUR IMPACT AS A PRIVACY AND
COMPLIANCE LEADER BY EARNING YOUR
M.S. IN CYBERSECURITY & DATA PRIVACY.
NO J.D. REQUIRED.**

SPECIALIZED STUDY TAUGHT BY INDUSTRY EXPERTS IN THE FIELDS OF:

- Cybersecurity & Data Privacy
- Financial Compliance & Risk Management
- Government Affairs & Advocacy
- Health Law & Healthcare Compliance
- Human Resources: Law, Leadership, and Policy



**Enroll today to start
classes this summer!**

albanylaw.edu/graduate

2023 SESSION DESCRIPTIONS

DAY 1, June 6
11:00am-11:50am

What is Zero Trust?

Jeffrey Baez, Splunk

Zero trust is a philosophy and practice of network data security that assumes every user, device and service that attempts to connect to an organization's network is hostile until proven otherwise. The fundamental principle of zero trust is to secure an organization's data wherever it might live, allowing only legitimate users and entities access to relevant resources and assets. The modern data landscape includes cloud or SaaS deployments, data centers, remote workforces, mobile devices and a myriad of apps, which can no longer be protected by traditional security strategies. Allowing data and workloads to live, operate and be accessed in this expanded attack surface leaves many organizations increasingly susceptible to a host of security vulnerabilities and access issues. This problem was only compounded by industry-wide responses to COVID-19, in which companies moved quickly to support an all-remote work environment.

Case Studies Applying Machine-Learning in Cybersecurity

Eric Dull, Deloitte

Jeffery Janies, Deloitte

Machine-Learning is a toolset that has many applications in cybersecurity, including threat detection, unknown behavior identification, threat intelligence, report generation, and behavior categorization. Using machine-learning isn't simple or easy, and successful application requires use case and tool understanding, broad data visibility, and flexible computing environments. We will share lessons learned successfully applying machine-learning to a variety of cybersecurity use cases. We will also discuss Generative AI and a perspective on where it can help in cybersecurity analysis and automation.

Building Cyber Resilience: Why Does It Matter, and How Can You Get Started?

Jim Richberg, Fortinet

In this talk, we will discuss why building cyber resilience is increasingly necessary for effective cybersecurity and explore how its benefits extend beyond cybersecurity. Building resilience is a focus of the new National Cyber Strategy and of operating principles, such as Zero Trust. The classic ingredients of people, process, and technology can be applied creatively and in multiple ways to solve this problem. This talk will explore some best practices and tips for building — and for funding — greater cyber resilience within organizations.

Why a Whole of Government Security Strategy Protects All New Yorkers

NYS Forum Information Security Workgroup

Join us for a panel discussion on enhancing government security strategy through collaboration. Learn how the challenges of government can be mitigated by effective partnerships and the utilization of industry resources.

2023 Verizon Data Breach Investigations Report

Neal Maguire, Verizon Cyber Security Consulting

Based on forensic evidence collected from our partner organizations, as well as the Verizon caseload, the 2023 Verizon Data Breach Investigations Report (DBIR) presents a rare and comprehensive view into the world of corporate cybercrime. Now in its sixteenth year of publication, this research has been used by thousands of organizations to evaluate and improve their security programs. The presentation will discuss the evolution of results over the years, and delve into the people, methods, and motives that drive attackers today. Attendees will learn about the most common attacks that affect their industry. You will learn about the actors who perpetrate these incidents, the techniques they use to carry out their attacks, the assets they prefer to exploit to gain entry into their victim's systems and networks, and the results of their actions. You will leave this session better equipped to make evidence-based decisions on the risks your organization faces on a daily basis.

**Tweet the conference at
#NYSCyber**

2023 SESSION DESCRIPTIONS

ASIA Session 1: Understanding Security Behavior

Paper: Development of Gig-Work Deviance Scale

Paper: Creating a Balance between Monitoring Practices and Flexible Work Arrangements

DAY 1, June 6
1:00pm-1:50pm

Zero Trust Cybersecurity Strategy for Government IT Leaders – How to Stay Ahead of the New Cyber Battleground

Tommy John, VMware

As they contend with growing security challenges and attack vectors increasing in size and scale, today's government organizations can become victims of malicious infiltration, and they may not even know about it. Though implementing Zero Trust solutions across their systems can often bolster defenses, questions remain on everything from improving visibility across these workloads to making more informed decisions across a broader cybersecurity ecosystem. In this session, we will discuss these issues and more, as well as learn how leading agencies are creating actionable insights for strategies on collaboration, risk mitigation, and everything in between.

Attendees will leave with an understanding of:

- How to evaluate cybersecurity progress and posture within their organizations.
- Strategies for eliminating blind spots with lateral security.
- The ways to prepare your organization to make zero trust or defense-in-depth efforts successful.

Re-energize with a
beverage and snack!

Afternoon Breaks sponsored
by CBTS and Check Point

June 6 at 3:00 pm – 3:20 pm

June 7 at 3:00 pm – 3:20 pm

How AI Embeds Human Bias and Distorts Our Decision Making

Antony Haynes, Albany Law

Leading diverse organizations not only requires consciously engaging human beings and culture but also requires carefully selecting and evaluating what automated systems are employed in all aspects of decision-making. Technologies ranging from resume scanners to language translation, from face recognition to criminal sentencing software, all encode and perpetuate biases present in human society. These systems show we cannot program away human prejudice by blindly relying on computer code. The purpose of this talk is to raise awareness of the ways computer algorithms reflect the biases of their human designers and to present a call to action for a code of ethics and for benchmarking standards around automated decision making systems.

Beyond Layers: Achieving Holistic Cybersecurity Through Tool Integration

Ryan Young, Vandis

In today's interconnected world, cyber threats are more prevalent than ever, and businesses need to have a comprehensive approach to security to ensure they are protected against cyberattacks. Defense in depth cybersecurity practices involve multiple layers of defense that can prevent attacks from gaining a foothold in a network. However, having multiple layers of defense is not enough. It is essential to have the right tools in place that integrate with each other, provide the necessary visibility and reporting, and work seamlessly to protect your organization. In this presentation, we will discuss the importance of integrating security tools to interface with each other and ensure proper visibility and reporting from all your tools. We will explore how leveraging an in-house SIEM solution or partnering with a third-party SOC or MDR platform can help you achieve this. We will also provide examples of how this approach can help detect and respond to cyber threats more effectively, reduce risk, and increase overall cybersecurity posture. Join us for this informative and educational presentation on defense in depth cybersecurity practices and the importance of integrating security tools for better visibility and reporting. We will equip you with the knowledge and tools necessary to safeguard your business against cyber threats and ensure a secure and resilient infrastructure.

2023 SESSION DESCRIPTIONS

How I Learned to Stop Worrying and Love My AI Overlords: Ethics and AI in Data Protection

F. Paul Greene, Harter Secrest & Emery LLP

The genie is out of the bottle. For better or worse, AI is here and its implications as of yet unknown. Whether it's used to write a term paper, identify and eliminate a target with a drone strike, or write your next Acceptable Use Policy, AI brings with it questions of agency, authenticity, identity, and ethics, all of which have strong implications for the field of data protection. This session will explore the emerging field of AI, whether it's algorithmic decision making, machine or deep learning, or any of the various ChatGPT iterations, and its implications for data security and data protection more broadly. In this regard, AI resides at the intersection of privacy, security, authentication and identity, policy, automation, and accountability, offering solutions, and risks, to some of our most pressing data protection concerns. We will discuss approaches to ethical AI, unethical AI use cases (whether intentional or otherwise), and assess real-life risks created by a tool that will soon become ubiquitous. Attendees will leave with a better understanding of what AI can, and likely should, do in relation to data protection under a number of regulatory and ethical regimes.

Threat Landscape and Resources

Elijah Cedeno, MS-ISAC

Cybersecurity challenges face all types of organizations. The threats we see impacting the private sector are similar to the threats that the MS-ISAC has seen impacting State-Local-Tribal-and Territorial entities throughout New York State. These threat actors are not only after money, personal information, and organization secrets, but they are also looking to damage your organization's reputation. While no single organization can prevent these threat actors from targeting and infiltrating your network, there are resources provided at no-cost that can help mitigate these risks. Resources ranging from actionable intelligence and passive monitoring of your public information, to actively blocking malicious connections from establishing, are available at no-cost to over 15,000 organizations across the United States. During this presentation we will discuss the current threats impacting New York State and resources are that can minimize and mitigate these threats.

ASIA Session 2: Privacy Breaches

Paper: Investigating HIPAA Cybersecurity & Privacy Breach Compliance Reporting during COVID-19

Paper: Privacy Paradox: Is it really a paradox?

DAY 1, June 6
2:10pm-3:00pm

How Breaches Should Shape Your Zero Trust Strategy

Jeremiah Salzberg, CDWG

Zero Trust has become the big buzzword in the Information Security industry. However, Zero Trust is MUCH more than just a buzzword. In this talk, we'll look at some recent breaches and discuss how a zero trust strategy/approach can help to limit the impact of a breach.

AI in Cybersecurity: Navigating the Hype and Making Informed Decisions

Dean Maloney, GreyCastle Security

Hiring and retaining cybersecurity professionals is increasingly more complex, forcing companies to implement artificial intelligence to relieve the burden through automation. While AI offers real benefits today, it requires continued analysis and human expertise to understand cybersecurity's impact and limitations. Join us for a look at new emerging AI technologies, how to navigate the artificial intelligence hype, and how to make informed decisions that help secure you and your customers.

Learning Objective #1: Define artificial intelligence, distinguish its distinct types, and recognize its purpose & common applications in current cybersecurity technologies.

Learning Objective #2: Characterize the new emerging AI technologies that will become commercialized in the next 1-3 years.

Learning Objective #3: Evaluate the efficacy and limitations of artificial intelligence's current commercialized capabilities through a provided scorecard when looking to include or expand them into your existing cybersecurity architecture or plan.

Learning Objective #4: Design a comprehensive plan addressing your organization's top risks and threats that integrates human expertise and artificial intelligence.

2023 SESSION DESCRIPTIONS

A Brave New World: An Exploratory Look Into the Next Century of Hacking and Cybercrime Tactics

Tyler Wrightson, Leet Cyber Security

What it will mean to be human and face the cybercrime challenges of the next century. Deep fakes, artificial intelligence, voice cloning, biometrics, robotics, holograms, cryptocurrency, smart contracts, smart devices, smart homes, smart cities, IOT: how do they all play a part in the safety and security of humans, and what will ransomware, malware, extortion, and kinetic attacks look like in the future? This is not a practical talk about what to do today, but rather an exploration of the crazy things that will happen over the coming years as technology continues to evolve and hackers and cybercriminals look to take advantage of it for their own profit.

Data Security: Common Misconceptions with Immutability & Recovery | Managing Endpoint Risk at Scale

Liam Kearns, Tanium

Shawn McElhinney, Rubrik, Inc.

In Part 1, you will hear how public sector customers still find themselves not being able to successfully recover their environments after a cyber attack. This discussion will focus on what constitutes as “immutability” and how that can impact obtaining/lowering cyber insurance and ensuring a successful recovery in a short amount of time.

In Part 2, you will hear how tool complexity, expanding digital experience initiatives and hybrid working environments are increasing organizational risks today. This technical conversation will focus on how linear chain architecture can simplify the management of today's risk, no matter where endpoints reside and at any scale.

Business Email Compromises: An Evolving Attack

Courtney Dayter, Kroll Cyber Risk

Jamie Vendel, Kroll Cyber Risk

Throughout the last decade, cyber crime has continued to evolve and change, bringing many new attacks to the forefront of cybersecurity. While phishing has long been recognized as a significant security issue, Kroll's investigations show that it is evolving to become an even greater threat. Kroll threat intelligence data that shows that phishing attacks increased by 122% in 2022. With the change of the year came a rise in usage of more advanced tactics, techniques and protocols. Kroll has seen a prevalence of attacker in the middle (AiTM) and advanced phishing emails, including domain name spoofing and multifactor authentication. Kroll's presentation will explore methods used to gain access to a mailbox, establish persistence, toolkit development and mission execution within Business Email Compromises (BEC). BEC are a leading type of cyber attack that target organizations with the goal of stealing money or information. Kroll will provide guidance on how to improve email hygiene to protect your organization.

ASIA Session 3: Active Defense

Paper: Honeypots and Honeytokens in Active Defense

Paper: Exploiting hacker biases to Thwart Hackers

**DAY 1, June 6
3:20pm-4:15pm**

An Introduction to Zero Trust Architecture

Richard Conklin, Accenture

In the digital era, security teams are struggling to maintain control of the attack landscape, and it's going to get harder. Perimeter-based network access was designed in a different time, for a different problem. As the problem is expected to persist, a new approach is required. The Zero Trust Model is changing how access is granted. In this session, attendees will receive an introduction to and a unique perspective of Zero Trust Architecture. You will learn the attributes of the Zero Trust security platform, prevailing client challenges and solutions, typical outcomes with Zero Trust security, as well as various deployment and governance models. You will also review industry frameworks and recommendations, client and vendor responses and common starting points for clients.

Google Cloud is keeping
attendees hydrated as the
2023 Water Station Sponsor.
Thank you!

2023 SESSION DESCRIPTIONS

AI-Machine Learning-Data Management Governance & Controls Cloud Computing Best Practices: CNY Quantum Valley Pentagon-USAF-USSF Ventures Spanning Air-Space-Cyberspace-Outer Space

Yogesh Malhotra, Global Risk Management Network, LLC

Our CNY Quantum Valley AI-Machine Learning-Data Management (AI-ML-DM) Governance & Control Cloud Computing practices build on a 30-year foundation of sustainable digital systems and networks practices leadership, R&D ranked for impact among AI-Quant Finance Nobel laureates, and applied global industry benchmarks for self-adaptive complex systems and chaos engineering as the digital transformation pioneer profiled in *Business Week*, *Computerworld*, *CIO Magazine*, *Fast Company*, *Fortune*, *Inc.*, *New York Times*, *Wall Street Journal*, etc. Our Digital CEO-CxO (CEO, CIO, CTO, CISO, CSO, CDO, CRO, CFO) leadership practices in sustainable cloud computing address three interrelated applied problems in an integrated manner:

- a. Complex systems fail all the time;
- b. Cybersecurity is job zero for AI-agility and cyber-resilience, and
- c. Managing dynamic and adversarial uncertainty is critical for sustainability.

Solving this 'trilemma' is essential for designing, building, and sustaining self-adaptive digital systems and digital networks spanning the world, as well as for CNY Quantum Valley Pentagon-USAF-USSF Ventures spanning air-space-cyberspace-outer space. As sustainable digital systems and digital networks pioneer, we lead risk mitigation of complex systems failures as self-adaptive complex systems and chaos engineering pioneers of human-centered AI systems, human-centered search, and human-centered networks advancing the human-centered world wide web.

Building on our AI-ML-DM governance and control/risk management cloud computing practices, as well as Pentagon Joint Chiefs, guidance 'Beyond ABMS-JADC2' spanning Air-Space-Cyberspace-Outer Space, with invited interviews for Pentagon USAF Chief Scientist while serving on Pentagon USAF C4I-ISR CTO-DoD CIO Team as Chief Data Scientist, we will share with you the latest advances in the AI-ML-DM governance and control cloud computing practices advancing on 30-year 'Big 3-Cloud Computing' practices leadership.

ChatGPT – Yes, It Generates Code...but Is It Secure? Leveraging Machine Learning and Artificial Intelligence tools with Application Security Scanning

Chris Wysopal, Veracode

With the evolution of Artificial Intelligence (AI) and the ability to develop an application at the press of a button, attendees will receive key insights into application security, machine learning and ensuring government services are secure. Focusing on speed to deliver secure code, you will hear new techniques, auto remediation based on machine learning and best practices to leverage automation.

The Five Essentials of Ransomware Prevention

Chris Jensen, Tenable

To achieve optimal network security, you must implement a proactive and comprehensive approach to make your network a "hard target" capable of defending against ransomware and other damaging cyber attacks. In this presentation, you will learn five essential components of effective cyber defense, including the following:

1. Know your entire network – you cannot protect it if you don't know it is there.
2. Implement a dynamic, proactive vulnerability management program based on actual risk.
3. Choose the right security tools and use them for their intended purposes.
4. Look at your network from the attacker's perspective.
5. Secure and proactively monitor your Active Directory to enable timely incident response and minimize damage in the event of a cyber attack.

ASIA Session 4: Cybercrime and Hacking

Paper: Improving Ethics Surrounding Collegiate-Level Hacking Education

Paper Investigating Cybercrime Using Code Authorship Analysis & 4P Forensic Conceptual Model

Passport Raffle

Visit our exhibitors for a chance to win some amazing prizes. Bring the Exhibitor Passport to each of the listed booths and have it stamped; it's that easy! Once the passport is stamped, please bring it to the Registration Table. Drawings will be held during the 3pm break on Tuesday, June 6 and Wednesday, June 7. Prizes must be picked up by the end of the conference. The passport is made possible by generous donations from our conference sponsors and exhibitors.

The Conference is proud to support cybersecurity education.

The NYS Cybersecurity Conference Scholarship helps provide scholarship opportunities to University at Albany students with a demonstrated interest in cybersecurity.

**Congratulations to
the 2023 recipients:**

Angelica Hernandez
Jason Moon

2023 SESSION DESCRIPTIONS

DAY 2, June 7
11:00am-11:50am

The Importance of Incident Response Testing: This is NOT a Drill

Daniel J. Altieri, Harter Secrest & Emery, LLP
Laura K. Schwalbe, Harter Secrest & Emery, LLP

The ever-present danger of ransomware incidents, phishing attacks, and hacking demand strong preparation practices. It is difficult to prepare for incident response in a vacuum, as many incidents involve issues that an organization may be seeing for the first time. This workshop demystifies the incident response process and includes abbreviated, real-world scenarios. Attendees will engage in realistic real-time discussion of important issues, such as Incident Response Plan structure and content, insurance concerns, communications strategies, and best practices for leveraging necessary stakeholders. The goal of the workshop is to provide you with tools to promote and inform incident response planning within your organizations.

iSECURE: How Organizational Culture Impacts Compliance!

Robert Adams, iSECURE, LLC

This is a presentation for cybersecurity professionals, including C-level and administrative stakeholders. Attendees will learn the impact of culture on the approach to compliance that organizations take. We will compare and contrast two organizations that are widely different in their approach to managing risk, due diligence and enforcement. Join us as we explore the Healthcare and Financial industry markets.

We Need a Compliance Control for Retaining Cybersecurity Professionals

Deidre Diamond, CyberSN

Organizations must examine risk through the lens of dire talent retention issues. Organizations have control over retaining talent, and yet the statistics are horrifying. Cybersecurity professionals are not happy with their current employment and move jobs regularly. Talent retention controls seem greatly necessary, being that organizations are not following best practices for retaining and or hiring cybersecurity professionals. This negligence puts an organization in a higher risk bracket, and therefore compliance control is greatly needed.

Resilience in a Cyber World – Three Critical Steps Towards a Mature Cybersecurity Program

Ryan Ettl, Infoblox

Many organizations are often faced with “staying ahead” of the latest cyber threats, understanding the most recent alerts, impacts of governmental compliance, and balancing operational priorities. With all these ever-present concerns, Security teams are rapidly overburdened with challenges that result from overlooking the foundational elements of cybersecurity. Attendees will learn how organizations can set the path to cyber success that’s flexible and endures dynamic cyber adversaries.

Cloud Security...On the Cheap

Randy Wheeler, NYSTEC

Christie Hall, NYSTEC

Cloud computing has changed the IT landscape for the better by providing access to elastic resources that can fit your budget, even if your organization is quite small. But let’s face it, cloud computing is complicated, and it can be difficult to know who is responsible for what and how to provide assurances that someone did not accidentally permit unauthenticated access to your sensitive data. Each cloud vendor does things differently and getting a handle on where to focus security compliance efforts on a small budget can be overwhelming. We like to say that “cloud security is easy to get right but also easy to get wrong.” These challenges begin with procurement and end with confirmation that your data was deleted when it needs to be, and all the computing in between.

In this session, attendees will receive an overview of the abundance of free resources available from organizations like NIST, CISA, CIS, CSA and cloud vendors themselves that will arm you with control baselines, share responsibility guidance, assessment methods and favorite adversarial attack points that can inform your procurement approach as well as cloud security responsibilities. You will learn how to leverage these resources in your organization and the only thing it will cost you is time. This presentation will include a take-home “cloud security on the cheap” reference guide.

ASIA Session 5: Vulnerability Assessments

Paper: Reliability of CVSS Scores in influencing security decisions

Trusted security for government



The bridge to possible

Cisco.com/go/cybergov

2023 SESSION DESCRIPTIONS

DAY 2, June 7
1:00pm-1:50pm

DevSecOps Explained

Neil Pathare, Synopsys

DevSecOps is a trending practice in application security that involves introducing security earlier in the software development life cycle. It expands the collaboration between development and operations teams to integrate security teams in the software delivery cycle. DevSecOps needs to be risk-based like your application risk indicator. It needs to be able to optimize security testing based on your policies. It should be efficient so not every code change requires a full security analysis. In this talk, attendees will learn actionable insights into what DevSecOps is, what DevSecOps is not, and how DevSecOps works from build to production.

Number One Risk: Not Knowing Your Asset Inventory

Aaron Anderson, JANUS Associates

Number One Risk: Not Knowing your Asset Inventory will focus on Attack Surface Discovery (ASD). ASD can help an organization address the growing shadow IT problem by identifying rogue assets, and by significantly reducing cost, waste and cyber risk all while ensuring compliance and improving overall asset awareness. Today, organizations struggle to manage their IT assets with 30-40% of all deployed technology spending not appropriately managed or secured in accordance to the organizations policy. ASD addresses this concern by gathering intelligence on the organizations public facing assets and by assessing the organizations exposure to attack and data leakage.

Attendees will learn about Shadow IT and how to identify external facing assets that are unknown to the organization. In addition, you will also take home expert advice on how to reduce the attack surface and associated asset waste and blind spots.

Methods and Tools to Help Grow and Keep Current Cyber Employees

Susie Kendis, Deloitte

Mara Patashnik, Deloitte

State and local cybersecurity organizations compete in a war for talent, as demand outpaces supply and private sector companies offer candidates enticing work options. In November, New York State Empire State Development (ESD) reported that "New York State ranked the #3 U.S. market for cybersecurity jobs, with New York City in second place," based on LinkedIn data. With limited resources and overburdened HR support teams, we help cyber teams be purposeful in how they retain and develop existing talent.

Attendees will learn methods and tools for cyber teams and employers to develop and engage current employees in order to help grow and keep them, to enhance their effectiveness, and to convert them into brand ambassadors. Recognizing the challenges of hiring, we focus on the other parts of the hire/retain/develop framework, including the employee experience, internal communications, and organizational culture. You will walk away with tangible, low-budget tactics which can be implemented to support and maximize the experience of your existing employees — all to supplement ongoing recruiting activities.

Building Stronger Cybersecurity Communities: Driving Awareness and Training for a More Secure Digital World

Kiran Bhujle, SVAM International Inc.

Shahryar Shaghaghi, SVAM International Inc.

Cybersecurity is a critical concern for individuals and organizations alike, and building awareness and providing training is essential to creating a secure digital environment. Attendees will learn the importance of community-building in driving cybersecurity efforts, as well as the benefits of creating a security culture and leveraging a community's collective knowledge and skills. You will also examine effective strategies for increasing cybersecurity awareness and providing training, such as conducting regular security assessments, implementing security protocols, and creating user-friendly training programs.

Thank you to NYSTEC for
sponsoring lanyards for
the 2023 NYSCSC!



Cyber for the frontline

Where does cyber fit in your operations? At the frontline. Through our technology-enabled cyber and strategic risk services, trusted advice, and relentless focus, Deloitte helps clients navigate a fluctuating world of risk and opportunity. We enable government and public service organizations to lead through uncertainty while driving outstanding and sustainable performance.

www.deloitte.com

Copyright © 2022 Deloitte Development LLC. All rights reserved.



2023 SESSION DESCRIPTIONS

Trends in Cloud Security

Sailesh Gadia, KPMG LLP

While it may seem that cloud security has matured, the reality remains that this space is constantly evolving. Inherent benefits of cloud have led organizations to seek new ways to leverage it, from use of Cloud for Disaster recovery to Artificial Intelligence models. Attendees will learn of the latest tools and techniques for designing and operating cloud security in a multi-cloud environment. This session will also include a discussion on the learnings from Cloud migrations based on our work with large complex organizations.

ASIA Session 6: Phishing and Deception

Paper: Too Much of a Good Thing: Examining Politeness Cues on Phishing Email Detection

Paper: Beyond the Human Eye: Comprehensive Approaches to AI Text Detection

DAY 2, June 7
2:10pm-3:00pm

Cyber Defense Lessons From Ukraine

Anita Biernat, Utica University

The Russian invasion of Ukraine in 2022 has tested under real-world conditions many best practices in cyber defense. For the better part of a decade, government executives, industry professionals, and researchers have all emphasized the importance of public-private sector cooperation, international partnerships, and flexible, timely intelligence sharing in cybersecurity, for example. Attendees will learn how these ideas have been evident in the conflict in Ukraine and demonstrate that the past decade's conventional wisdom has held up remarkably well in the midst of this ongoing war.

Privacy Primer: Tips for Building, or Updating, Your Privacy Program

Michele Warner, NYSTEC

Jeffrey Wilson, NYSTEC

That organizations will continue to collect, use, and retain personal information that could be used to identify us as specific individuals is a fact of modern life. This information allows an organization to fill orders, pay employees, and conduct all aspects of business. But when such information is misused either intentionally or accidentally — it can cause irreparable harm. Because of this, the rules governing what information organizations may collect, and how they may use and retain it, are evolving quickly, as governments across the globe move to give people more control over their own information. The broad reach of the European Union's General Data Privacy Regulation (GDPR) has affected privacy around the world. The California Consumer Protection Act (CCPA) may provide clues about future domestic privacy policy. While New York State and the federal government have not yet passed comprehensive privacy laws, they surely will. How will these anticipated changes affect individuals and businesses? Attendees will receive some insight to help you and your organization read the tea leaves, and design a new or update your existing privacy program to support your business and its customers, understand how to think about the evolution of privacy laws and regulations, and determine a sensible approach for implementation.

Cyber Crime — Challenges and Solutions

Carl Mazzanti, eMazzanti Technologies

Cybercrime is big business. In 2022, the FBI's Internet Crime Complaint Center (IC3), recorded more than 800,000 complaints, with losses totaling \$10.3 billion. Attendees will receive an incisive overview of this critical topic, with highlights that include:

- What is cyber crime (sociology of hacking, and monetization of the hack; and cloud security (protection that the cloud can, and cannot offer?
- A brief look at some additional legal exposures that can be triggered by a hack (Regulatory and Compliance Requirements: HIPAA, PCI, other)
- Tips to design systems, policies and configurations that are so tight that a cyber insurance policy will hopefully never be needed
- Step up your business' protection with contingency planning and testing (Business Testing/Disaster Recovery/Incident Response)

2023 SESSION DESCRIPTIONS

How Organizations “Stay Ready So You Don’t Have to Get Ready”

Erik Gaston, Tanium

For CIOs & CISOs, the current IT landscape is challenged by lack of visibility and no clear understanding of what is required to get in a constant state of readiness to manage more proactively. Attendees will learn of practical ways to help their IT organization “stay ready so they don’t have to get ready,” a proactive approach to dealing with cybersecurity and operational management/risk issues. You will learn how to establish key programs and the critical questions that every leader needs to ask and answer daily.

Making Sense of the Wild West of Digital Identity

Ames Fowler, ForgeRock

Marcin Zimny, ForgeRock

This session will provide attendees with a lighthearted yet informative look into the world of digital identity, using a wild west metaphor to explain important concepts to cybersecurity team members and other roles across the IT organization. By the end, you will have a basic understanding of the core elements of digital identity and a foundation for further exploration. This session will illustrate concepts that support the main pillars of digital identity, including trust, authority, delegation, and federation, as well as their role in the typical user login experience. This unique presentation takes a metaphorical look into digital identity following the adventures of a newcomer to the wild west town of “El Dap,” where the town is being challenged by a gang of bad actors. Parallels are drawn between the relationships of the townsfolk and trusted establishments (bank, town hall, sheriff, saloon, and others). In this construct of the wild west, we simplify the notions of registration, authentication, multi-factor authentication, authorization, trust, privileged access management, and the associated technologies behind them: tokens, certificates, SSL, SAML2, OAuth 2.0, OIDC, and others.

ASIA Session 7: Covert Channels

Paper: Introducing a Novel Covert Channel Into Backgammon

Paper: Covert Channels in Cryptic Crosswords

DAY 2, June 7

3:20pm-4:15pm

The Three Pillars of Email Authentication

Joseph Maltino, Spruce Technology

Nicolas Villacis Vukadinovic, Spruce Technology

Email authentication through SPF, DKIM, and DMARC is important to prevent email fraud, phishing attacks, and email spoofing. These three protocols work together to authenticate the sender’s domain and ensure that only authorized mail servers can send emails on behalf of the domain. This layered defense helps to build trust between email senders and recipients, reducing the risk of falling victim to scams and malicious attacks. DMARC also provides visibility into email authentication failures and helps to prevent phishing and spoofing attacks by allowing domain owners to specify what actions should be taken when an email fails authentication checks.

What Do the New FTC Safeguard Rules Require You to Do in 2023?

John Bruggeman, CBTS

The FTC has established new safeguards for organizations that are significantly engaged in financial activity with their customers, but what does that mean? Attendees will learn the new rules below and how they apply to organizations.

1. Designate a qualified individual to supervise the Information Security Program.
2. Create, maintain, and manage an Information Security Program.
3. Create and maintain a written Risk Assessment of the environment.
4. Establish and maintain a written Incident Response Plan.
5. Design and implement safeguards to control the risk.
6. Train and educate staff.
7. Oversee and monitor service providers.
8. Regularly test or monitor the effectiveness of safeguards, like test access controls, vulnerability management and penetration testing.

2023 SESSION DESCRIPTIONS

Anatomy of a Cyber Attack

Dennis O'Connell, Custom Computer Specialists

Using real life examples, attendees will walk through cyber attacks that have occurred in our region and we'll review how the organizations responded and recovered. You will learn of the difference responses required for not-for-profit and for-profit entities. You will also learn the importance of a well-defined plan, along with tips on how best to handle an attack, because while we may not always be able to prevent an attack, we can always be prepared.

Creating a Cybersecurity Roadmap for Schools to Protect K-12 Students, Teachers and Parents

Richard Cocchiara, CxO Expertise

Today's data in any organization is at risk, but even more so for schools where students may not know their data has been stolen for years to come. Most parents don't even think about cybersecurity protection for their children. However, there are criminals and sexual predators that are always looking to get into any K-12 school system. Using his over 25 years of consulting experience, Richard Cocchiara was tasked with taking over as Chief Information Security Office to help put the NYC Department of Education on a path to cybersecurity protection.

In this session, attendees will learn of the steps taken to protect the largest school system in the country, including the steps he took to analyze, design and plan for improved cybersecurity. You will hear practical, real-life lessons from someone who has been there and done it.

How to Secure Active Directory: Best Practices for Detection, Remediation, and Recovery

Steve Walker, Semperis

Cyberattacks are the most critical threat facing modern information technology. Most attacks start with identity compromise. For the past quarter century, identity in the enterprise has been synonymous with Microsoft Active Directory (AD). Therefore, AD is almost always involved in a cyberattack—either as the target or as a route to the target. AD is a marvelous service. But its age, as well as vulnerabilities that accumulate over time, make it highly vulnerable to threat actors. Once compromised, AD is extraordinarily difficult to recover. Attendees will:

- Learn the top vulnerabilities encountered in AD, how to mitigate them with free tools, and the complications of AD recovery.
- Discover the most common AD vulnerabilities and misconfigurations.
- Learn why AD is the cyber kill chain's weakest link, exploited in virtually every modern attack.
- See how new cyber-first disaster recovery technologies automate the recovery of complex systems, facilitate recovery to the cloud, and eliminate the risk of reinfection from system state and bare-metal backups.
- Learn how to use free tools to reduce your AD attack surface.

ASIA Session 8: Covert Channels

Paper: Pragmatic Study of MQTT 5.0 Network Covert Channels

Don't forget to grab your official conference bag at registration.
CoreBTS is the 2023 NYSCSC Bag Sponsor!



Secure Government, Data Center to Edge

Cybersecurity, everywhere you need it.

www.fortinet.com



2023 CONFERENCE SPONSORS

TERABYTE:



Fortinet

Cybersecurity, everywhere you need it

FortiOS, Fortinet's operating system, is the foundation of the **Fortinet Security Fabric**, the industry's highest-performing and most expansive cybersecurity platform, organically built on a common management and security framework. FortiOS ties all the Security Fabric's security and networking components together to ensure seamless integration. This enables the convergence of networking and security functions to deliver a consistent user experience and resilient security posture across all manner of environments including on-premises, cloud, hybrid, and converging IT/OT/IoT infrastructure.

MEGABYTE:



Cisco

Cisco, the worldwide leader in technology that powers the internet, and the largest enterprise cybersecurity company in the world, has applied its unparalleled networking, data, and application expertise to provide an integrated, open platform of intelligent security products and services, supported by hundreds of third-party integrations. Save time, cut costs, and gain flexibility with built-in security that accelerates transformative IT initiatives, such as hybrid work, modern applications, and multicloud initiatives. Protect, detect, analyze, and respond everywhere with insights and assistive automation informed by the world's most extensive network telemetry, and largest commercial threat hunting team. Secure work wherever it happens with Cisco Secure.



Deloitte

Our people, ideas, technology and outcomes – are all designed for impact. Our team of over 20,000+ professionals across the country bring fresh perspective to help you anticipate disruption, reimagine the possible, and fulfill your mission promise. Whether you are at the crossroads of AI and workforce transformation, cyber and IT modernization or digital and citizen experience—we bring actionable insights to drive bold and lasting results. Deloitte's shared purpose and passion help you make an impact and improve the lives of New Yorkers.



Transform the government experience

Reach new heights with Amazon Web Services by delivering mission-critical services

Learn more ›
aws.amazon.com/stateandlocal



Make Application Security Easy

F5 and WorldTech IT are proud Kilobyte Sponsors for the 2023 New York State Cyber Security Conference!



F5.com
wtit.com

2023 CONFERENCE SPONSORS

KILOBYTE:



Amazon Web Services (AWS)

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. Public Sector organizations of all sizes use AWS to build applications, host websites, harness big data, store information, conduct research, improve online access for citizens, and more. AWS has dedicated teams focused on helping our customers pave the way for innovation and, ultimately, make the world a better place through technology.



F5/WTIT

At F5, our mission is based on the fact that governments depend on applications. F5 ensures applications are always available and secure, anywhere. The world's largest government entities rely on F5 to stay ahead of security, cloud, and mobility trends. WorldTech IT is the leader in Professional & Managed Services around F5 and NGINX. A top-tier F5 Guardian Partner for application delivery, automation, and security; our services around F5/NGINX also include Microsoft, Red Hat, and Public Clouds. Try Cloud.Red – our F5/NGINX Monitoring, Alerting, Observability, and Central Management solution.

The 2023 NYS Cybersecurity Conference would like to thank all of our sponsors, exhibitors, speakers, volunteers, and attendees for making this another successful year!



Zero Trust
Data Security™

RUBRIK FOR STATE & LOCAL GOVERNMENT

Data Protection & Security for the New Norm

Rubrik delivers a radically simplified approach to data management for state & local governments to recover from ransomware attacks, accelerate cloud mobility, and streamline operations in this new norm.

Learn More @ www.rubrik.com/industries/state-local-government

Don't Backup. Go Forward.



ENABLING DIGITAL TRANSFORMATION THROUGH INNOVATION, TRUST AND SECURITY

Providing secure, scalable and reliable IT solutions for seamless business operations

Cyber Security

Cutting-edge security solutions to minimize or mitigate unauthorized access and breaches. 24/7 support across the globe.

Custom Application Development

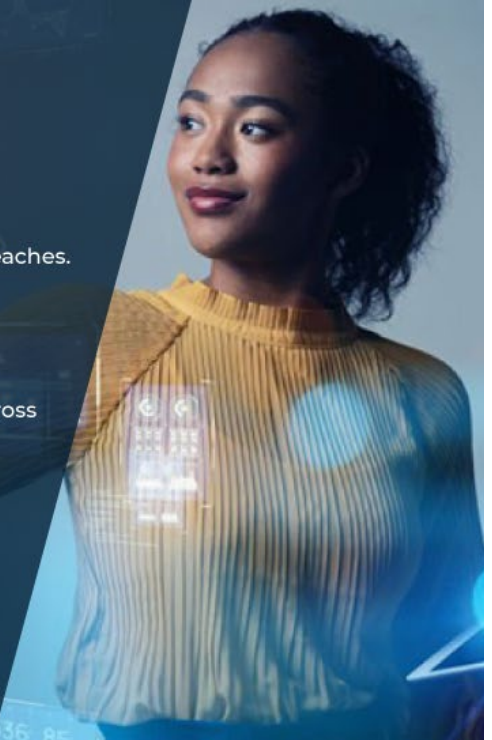
Bespoke secured software solutions with a targeted approach to problem-solving across the organizations.

RPA

Intelligent & Secured automation of repetitive tasks to minimize human error and maximize value.

Consulting and Staffing

Rigorous and focused screening methods to find the right match for an organization's staffing needs.



To know more, visit: www.svam.com

2023 CONFERENCE SPONSORS

KILOBYTE:



rubrik

Rubrik

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. Our platform automates policy management of data and enforcement of data security through the entire data lifecycle. We help organizations uphold data integrity, deliver data availability, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.



SVAM

INTERNATIONAL, INC.

SVAM International

SVAM International is a global technology and consulting firm focused on digital transformation to bring value through simple, modern and secured digital solutions. SVAM specializes in modernizing legacy applications, automating IT workflows, and securing IT systems through emerging technologies that improve customers' experience and engage them better. As a leading provider of IT support and related services across multiple countries in the world, SVAM believe that innovative technologies are the lifeline of businesses and therefore, we are committed to providing comprehensive, business-focused solutions like app modernization, data analytics, RPA, cybersecurity, consulting and staff augmentation services, and managed services.

Please take a moment to provide feedback via the mobile app at the end of each session you attend, as well as at the conclusion of the conference. We value your comments.



Proud sponsors of the NYS Cybersecurity Conference

Complexity Minimized with ThunderCat Technology



Supply Chain Services



Integration & Staging Facility



Managed Services



Other Services

www.thundercattech.com

Endpoints Secured with Tanium



Visibility



Control



Remediation

www.tanium.com/slq



Protect your business from cyber threats with **Trend Micro's leading enterprise-grade cybersecurity solutions**. Our advanced technology and expert support will keep your sensitive data and systems safe from attacks.

Stop by **booth #12**
to learn more



2023 CONFERENCE SPONSORS

KILOBYTE:



ThunderCat Technology/ Tanium

Tanium and Thundercat are partners supporting the technology needs for the State of New York. ThunderCat Technology is a Service-Disabled Veteran-Owned Small Business (SDVOSB) that delivers technology products and services to government organizations, educational institutions, and commercial enterprises. We are a VAR that brings an innovative approach to solving customer problems in and around the datacenter by providing strategies for infrastructure, cybersecurity, and cloud transformation. Tanium, the industry's only provider of converged endpoint management (XEM), protects every team, endpoint, and workflow from cyber threats by integrating IT, compliance, security, and risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. State and local governments and educational institutions trust Tanium and Thundercat to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere.



Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to simplify and secure their connected world. **[TrendMicro.com](https://www.trendmicro.com)**

Join us for a Continental Breakfast each morning in the Exhibit Hall!

June 6 breakfast sponsored by Cisco

June 7 breakfast sponsored by Deloitte



Your Cybersecurity Partner in:

- Vulnerability Assessments
- Cloud Security Assessments
- Penetration Testing
- vCISO
- Managed Security Services
- GRC Assessment and Management
- Zero Trust Access
- Tabletop Exercises
- Cybersecurity software & hardware solutions

JOIN US AT OUR 13TH ANNUAL SUMMER CYBERSECURITY CONFERENCE JULY 27TH - ROCHESTER NY

Explore how today's cybersecurity world aligns with the secrecy and culture of the past at our *Speakeasy Parallel*.

passwords
secret culture
rules of entry



hidden entrances
organized crime
ransomware

This year's keynote speaker is Bob Kalka, VP Executive at IBM.
He'll reveal the top dirty little secrets that CISO's haven't been telling you!

Contact us!

354 N. Goodman Street
Rochester, NY 14607
585.419.8200



Scan the QR Code
to register for the event!



2023 CONFERENCE SPONSORS



Bag Sponsor

Core BTS

Core BTS is a full-service digital transformation consulting firm. We can meet clients wherever they are at on their digital journey and help them chart a clear path forward. We solve their most pressing challenges by delivering integrated solutions that connect people, process, and technology to defined business outcomes.

Lanyard Sponsor

NYSTEC

NYSTEC is an independent nonprofit technology consulting company, advising organizations, agencies, institutions, and businesses since 1996. We help clients plan and manage the acquisition, implementation and security of their IT systems. With offices in Rome and Albany, NY, as well as New York City, NYSTEC employs proven processes for project management, business analysis and system integration to serve clients in many sectors, including the company's main client base, government. We are a trusted partner to government at the county, state, city and local level, advising our clients on how to use the right technology and helping them achieve real business outcomes.



Afternoon Break Sponsor

Check Point/CBTS

State and local governments possess a wealth of information on citizen activity and government operations, making them prime targets for cybercrime. To fend off cybercriminals, you need to look beyond traditional methods. The Check Point and CBTS partnership provides your organization with the necessary tools to secure your sensitive data and critical infrastructure. Delivering end-to-end security service offerings we help state and local organizations prevent advanced threats, respond to widespread attacks and enhance their security resilience strategy for their citizens.



Water Sponsor

Google

Google Cloud is helping state and local governments empower their workforce and improve the lives of their constituents with our secure, interoperable, intelligent platform. Whether your organization is looking to build new applications in the cloud or transform your current infrastructure, we can help modernize service delivery. <https://cloud.google.com/solutions/state-and-local-government>



2023 CONFERENCE EXHIBITORS

BYTE:



Advizex

Our deep heritage in both applications and hybrid infrastructure are essential elements of our approach to developing new solutions. Solutions that are designed to meet individual business needs.

For over 48 years we have partnered with our customers to “accelerate the adoption of new solutions to create business value.” Our passion for information technology is guided by our vision of: “Customers for Life.” www.advizex.com.



ALBANY LAW SCHOOL
ONLINE GRADUATE PROGRAMS

Albany Law School

Albany Law School's online graduate programs in cybersecurity and data privacy provide cybersecurity professionals and lawyers with the skills and knowledge to navigate the legal, regulatory, and policy landscape. Learn from faculty who are active practitioners and thought leaders in information security, data privacy, cybercrime, intellectual property law, and more. Be the bridge between technical teams, leadership, and legal. Study the latest issues and legal activity within the rapidly-evolving privacy landscape. A flexible online format allows students to balance their studies with their professional and personal commitments. It's still possible to apply for Fall 2023. To learn more, visit www.albanylaw.edu/graduate.



AUTOMOX

Automox

Automox is the cloud-native endpoint management platform for modern organizations ensuring every endpoint is automatically patched, configured and secured – anywhere, anytime. With the push of a button, fix critical vulnerabilities faster, slash cost and complexity, and win back hours in the day. Join thousands of companies transforming their IT into a strategic business driver with a single, cloud-native solution from Automox.



CLOUDFLARE

Cloudflare

Cloudflare is on a mission to help build a better Internet. Cloudflare's suite of products protect and accelerate any Internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. As a result, they see significant improvement in performance and a decrease in spam and other attacks. Today it runs one of the world's largest networks that powers anything connected to the Internet, with its services being used by everyone including state, local, and federal governments.

2023 CONFERENCE EXHIBITORS



Cribl®

Cribl

Cribl makes open observability a reality, giving you the freedom and flexibility to make choices instead of compromises.

Every organization has to deal with a myriad of challenges: scaling to keep pace with data growth, increasing cyberthreats, flat budgets, and a dearth of talent. In the face of these challenges, operations teams have been forced to make compromises.

The Cribl suite of products puts you back in control of your telemetry data, giving you the control to get the data where you want, and the flexibility to put it in any format you need on the fly. Learn more: <https://cribl.io/>



CROWDSTRIKE

CrowdStrike

Government institutions need a solution that protects against all cyber threats – simple and sophisticated. CrowdStrike a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. The CrowdStrike Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.



Custom Computer Specialists

Right People. Right Results.®

Custom Computer Specialists

Custom Computer Specialists is a leading provider of technology solutions and services to both public- and private-sector clients focusing on core software, managed services, IT consulting, cybersecurity, cloud, and network design and implementation. Our simple goal is to understand where our clients are on their technology journey and help them get to where they need to be. Founded in 1979, Custom's vast knowledge and experience make them a leading and trusted partner of educational institutions, healthcare organizations, nonprofits, and government agencies across the Northeast.

Custom has earned numerous awards including Best Cybersecurity, Best Computer Services and Best Places to Work.

DELL Technologies

Dell Technologies

Dell Technologies provides a unique approach through the **Dell** Trusted Infrastructure framework. This holistic, Zero Trust IT security approach encompasses the entire **Dell Technologies** portfolio and provides secure supply chain provenance, silicon-based security, secure software development lifecycle, and enterprise-grade management capabilities.

2023 CONFERENCE EXHIBITORS



DynTek

As a national systems integrator and risk management partner, DynTek delivers exceptional, cost-effective professional IT consulting services, end-to-end IT solutions, managed IT services, and IT product sales to state and local government, educational, healthcare and enterprise customers in the largest IT markets nationwide. Our broad range of technical expertise and vendor partnerships allow us to deliver solutions that support digital business transformation including **IT Security, digital infrastructure, modern workplace, data center and cloud** solutions. DynTek's multidisciplinary approach allows our clients to turn to a single source for their most critical technology requirements. For more information, visit <http://www.dyntek.com>.

EWASTE+
REGIONAL COMPUTER RECYCLING & RECOVERY

EWaste

EWASTE+ is a R2/RIOS Certified Electronics Recycling company and a licensed, NAID AAA Certified Data Destruction Contractor. EWASTE+ focuses on recovery of value from idle, obsolete and excess electronic equipment and operates a large-scale processing facility in Rochester, NY and two regional consolidation facilities in Albany and New York City. The company utilizes environmentally sound processing methods to maximize value and recovery while eliminating disposal of electronics in landfills

ExtraHop

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) helps agencies detect and respond to advanced threats—before they compromise your operations. We simplify and streamline investigations for known and unknown attacks by performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, agencies can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your mission and moving it forward, that's security uncompromised.

The Federal Bureau of Investigation

The Federal Bureau of Investigation is the principle federal law enforcement agency of the United States. In it's mission to protect the American people and uphold the Constitution, the FBI takes a lead role in protecting the United States from terrorist threats, cyber attacks, espionage and public corruption. If you'd like to learn more about working at FBI or partnering with FBI through InfraGard, please stop by.



2023 CONFERENCE EXHIBITORS



ForgeRock: One Platform. All Identities.

Improve the digital experience for your end users (citizens, residents, businesses) and government workforce with the modern Identity and Access Management (IAM) platform named a leader by top analyst firms. ForgeRock enables organizations to modernize, consolidate, and integrate legacy IAM systems. States including Texas, Utah, Connecticut, and California use ForgeRock to increase security, ensure privacy, and save costs. The ForgeRock identity platform can be consumed or deployed within any environment (on premises, cloud, hybrid-cloud, as a service). Learn more at www.forgerock.com.



Horizon3.ai

Horizon3.ai's mission is to help you find and fix attack vectors before attackers can exploit them. NodeZero, our autonomous penetration testing solution, is an unlimited, self-service SaaS offering that is safe to run in production, available on-demand, and requires no persistent or credentialed agents. See your enterprise through the eyes of the attacker, identify your ineffective security controls, and ensure your limited time and resources are spent fixing problems that matter. Not just a compliance checkbox; this is effective security. Founded in 2019 by industry, US Special Operations, and US National Security veterans, **Horizon3.ai** is headquartered in San Francisco, CA.



Infoblox

Infoblox unites networking and security to deliver better performance and protection. We provide visibility and control over who and what connects to your network and identify threats through intelligent DNS. Visit infoblox.com, or follow-us on [LinkedIn](#) or [Twitter](#).



iSECURE

Reimagining Cybersecurity

iSECURE

iSECURE was formed in 2011 and has solely focused on cybersecurity since its inception. Our mission is to inspire a Cybersecurity Culture through education and collaboration. iSECURE regularly host both in-person and virtual events to educate the community on top cybersecurity trends and utilizes intelligence, process, and experience to architect creative solutions that proactively protect each client. We are a trusted partner that specializes in:

- *Vulnerability Assessments*
- *Cloud Security Assessments*
- *Penetration Testing*
- *VCISO*
- *Managed Security Services*
- *GRC Assessment and Management*
- *Zero Trust Access*
- *Tabletop Exercises*
- *Cybersecurity software & hardware solutions*

2023 CONFERENCE EXHIBITORS



LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/ NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com/government



LP3

LP3 makes you the cyber and data hero by protecting your most sensitive data ensuring your organization has cyber resiliency, giving you peace of mind. Professional cybersecurity enterprise architects help you plan infrastructure service improvement on-premise or in the cloud.

Why do we do this work? Our national security matters. Over half of our employees are veterans. We eat and sleep national security. LP3 brings the lessons learned from the Intelligence Community and DoD to industry. We push hard to help prevent cyber issues from disrupting your mission critical operations. If our friends and neighbors, and the businesses we use, aren't secure, our nation isn't secure.



Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology— anywhere, on any device or app. Organizations trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, government, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. Learn more at okta.com.

Join us next year for the 26th
New York State Cybersecurity Conference!

2023 CONFERENCE EXHIBITORS



Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.



Premier Wireless

Premier Wireless is an elite T-Mobile partner and will be showcasing the latest in wireless technology and security. Stop by and meet the Premier and T-Mobile team.



QnA Tech

Established in 2009, Quality and Assurance Technology Corp, is an IT hardware, software, and services Value-Added-Reseller based in NY. We specialize in cybersecurity, anti-virus/spyware protection, data/disaster recovery, and breach remediation. We offer solutions from peripherals to data centers.

We are partnered with all the industry leaders to provide the best slate of options and offer all our end-users customized solutions.

Our team of IT experts have the technical know-how to keep your business safe and secure. We have years of experience working with some of the largest city agencies and government entities throughout the state.



Red Hat for State and Local Government

Red Hat's open source technologies help state and local agencies achieve their mission to serve citizens, respond to crises, and build public trust. We provide the support you need to deliver higher quality services faster—while improving the security, stability, and privacy of your systems. Red Hat's solutions can help agencies secure traditional and cloud workloads across all environments and secure and automate their infrastructure to reduce manual processes and security risks.

Red Hat is the world's leading provider of enterprise open source solutions—including Linux, cloud, container, and Kubernetes. We deliver hardened solutions that make it easier for enterprises to work across platforms and environments, from the core datacenter to the network edge.

2023 CONFERENCE EXHIBITORS



Repeat Business Systems

Repeat Business Systems is a full service premier office technology service provider with headquarters in Albany, NY and offices in Westmoreland, NY and Olean, NY. We sell and service copiers/printers/MFPs, plotters and production equipment, Quadient (Neopost) mailing machines, postage meters, folder-inserters, multi-carrier mailing systems, parcel lockers and VOIP phone systems. We also provide managed network services, network monitoring, backup and business continuity, security management and cybersecurity training.



Semperis

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada and Israel.



SHI

Think of SHI as your personal technology concierge. We connect your team with the IT solutions and services you need to support your organizational growth, security, and employee experience.



Spectrum Enterprises

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. Learn more at enterprise.spectrum.com



Splunk

Splunk is the data platform leader for security and observability. Our extensible data platform powers enterprise observability, unified security and limitless custom applications. Splunk helps tens of thousands of organizations turn data into doing so they can unlock innovation, enhance security and drive resilience.

2023 CONFERENCE EXHIBITORS



Vandis

Vandis provides Managed Services and IT Solutions to optimize the security and performance of network infrastructures, both on-premise and in the cloud. We design IT solutions to meet each organization's unique needs and goals. For nearly 4 decades, from SMB to enterprise clients, Vandis delivers comprehensive strategies for secure IT infrastructures.



Veracode

At Veracode, we offer a solution to integrate software application security into your software development life cycle. Our approach includes securing open-source libraries and educating developers for secure development. We also ensure compliance and connect your security and development teams, embedding our solution for vulnerability assessments and remediations. Our solution is scalable, integrates with development tools, and enforces security policies for your entire enterprise. We understand the complexity of software security, and our solution simplifies the process while providing comprehensive and effective security measures.



Vicarius

Vicarius helps IT and Security teams protect their most critical apps and assets against software exploitation through TOPIA, an autonomous end-to-end vulnerability remediation platform. Founded by three security experts and backed by tier-one investors from Silicon Valley, Vicarius' mission is to provide customers with problem-solving remediation solutions that proactively reduce risk wherever computer software resides. Learn more at <https://vicarius.io>



VMware

VMware, a leader in cloud infrastructure and enterprise mobility, delivering groundbreaking IT solutions. VMware's software-based approach to IT enables enterprises to accelerate digital transformation with Cross-Cloud Architecture(TM) and solutions for the data center, mobility and security.



Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.

PUBLIC SECTOR

THANK YOU TO ALL OUR 2023 CONFERENCE EXHIBITORS



Booth Assignments

| Company | Booth |
|-------------------------------|-----------|
| Lp3 | 1 |
| VMWare | 2 |
| QnA Tech | 3 |
| Crowd Strike | 4 |
| Thundercat/ Tanium – KILOBYTE | 5 |
| Cisco - MEGABYTE | 6, 7 |
| Conference Co-Hosts | 8 |
| Vicarius | 9 |
| AWS- KILOBYTE | 10 |
| Dyntek | 11 |
| Trend Micro – KILOBYTE | 12 |
| Albany Law School | 13 |
| SVAM International – KILOBYTE | 14 |
| Fortinet – TERABYTE | 15-16, 56 |
| Ewaste | 17 |
| Semperis | 18 |
| Veracode | 19 |
| Repeat Business Systems | 20 |
| FBI | 21 |
| Advizex | 22 |
| Arctic Wolf | 23 |
| Forgerock | 24 |
| Infoblox | 25 |
| Google | 26 |
| Rubrik – KILOBYTE | 27 |
| Cloudfare | 28 |
| Automox | 29 |
| Cribl | 30 |
| CBTS/Checkpoint | 31 |
| Red Hat | 32 |
| Splunk | 33 |
| Vandis | 34 |
| Okta | 35 |
| NYSTEC | 36 |
| iSECURE | 37 |
| Dell | 38 |
| Spectrum Enterprise | 39 |
| Acture Solutions, Inc. | 40 |
| Pure Storage | 41 |
| ExtraHop | 42 |
| LexisNexis Risk Solutions | 43 |
| Horizon3.ai | 44 |
| Premier Wireless | 45 |
| Microsoft | 46 |
| Palo Alto Networks | 50 |
| Zscaler | 51 |
| F5/ WTIT – KILOBYTE | 52 |
| Custom Computer Specialists | 53 |
| Deloitte – MEGABYTE | 54-55 |
| SHI | 57 |

